We claim:

1. A user authentication service for a communication network, comprising:

means for accepting and storing, as entries for particular users, user identification information;

means for accepting log-in responses entered on an end system, said system associated with a LAN interface in said network;

means for comparing for a match the accepted log-in responses with the stored user identification information; and

means for establishing network connectivity for the sytem if a match is found.

2. The user authentication service according to claim 1, wherein said LAN interface is operative for communicating with said system in a LAN media type.

3. The user authentication service according to claim 2, wherein said LAN media type is Ethernet or Token Ring.

4. A user authentication service for a communication network, comprising:

means for accepting and storing, as associated entries for particular users, user identification information and lists of network resources, said lists defining sets of resources operative in said network;

means for accepting log-in responses entered on an end system in said network;

means for comparing for a match the accepted log-in responses with the stored user identification information; and

means for establishing connectivity between the system and the defined set of resources associated with the matching user identification information.

5. The user authentication service according to claim 4, wherein said lists of network resources include identifiers of one or more virtual local area networks.

6. A user authentication service for a communication network, comprising:

means for accepting and storing, as associated entries for particular users, user identification information, time restrictions and lists of network resources, said time restrictions defining an access period, said lists defining sets of resources operative in said network;

means for accepting log-in responses entered on an end system in said network;

means for comparing for a match the accepted log-in responses with the stored user identification information;

means for establishing connectivity between the system and the defined set of resources associated with the matching user identification information, for the defined access period associated with the matching user identification information.

7. The user authentication service according to claim 6, wherein said lists of network resources include identifiers of one or more virtual local area networks.

8. A user authentication service for a communication network, comprising:

means for accepting and storing, as associated entries for particular users, user identification information, lists of network resources and enhanced authentication information, said lists defining sets of resources operative in said network, said enhanced authentication information identifying an enhanced authentication server operative in said network;

means for accepting log-in responses entered on an end system in said network;

means for comparing for a match the accepted log-in responses with the stored user identification information;

means for conducting an enhanced authentication session between the system and the identified enhanced authentication server associated with the matching user identification information; and

means for establishing connectivity between the system and the defined set of resources associated with the matching user identification information, if the enhanced authentication session is successfully completed.

9. The user authentication service according to claim 8, wherein said lists of network resources include identifiers of one or more virtual local area networks.

10. A communication network providing user authentication services, comprising:

n intelligent edge devices, where *n* is a positive integer;

an end system associated with each device, said system having means for communicating with said device;

a network management station, said station having means for communicating with said device;

means on said device for accepting log-in responses from said system and communicating the accepted log-in responses to said station;

means on said station for comparing for a match the accepted log-in responses with user identification information stored on said station;

means on said station for retrieving authorized connectivity information associated with user identification information which matches the accepted log-in responses; and

means on said station for communicating the retrieved authorized connectivity information to said device.

11. The communication network according to claim 10, further comprising means for accepting and storing, as associated entries, user identification information and authorized connectivity information for particular users.

12. The communication network according to claim 11, wherein said authorized connectivity information defines a set of resources operative within said network.

13. The communication network according to claim 10, wherein said authorized connectivity information includes identifiers of one or more virtual local area networks.

14. The communication network according to claim 10, wherein said authorized connectivity information defines a set of resources operative within said network and time restrictions.

15. The communication network according to claim 10, further comprising means on said device for using the communicated authorized connectivity information to establish and implement forwarding and filtering rules for packets transmitted to and from said system.

16. The communication network according to claim 10, further comprising means on said station for generating and storing user tracking information, said user tracking information including information relating to a single log-in attempt.

17. The communication network according to claim 16, wherein said user tracking information includes user identification information and information relating to the location of said system within said network.

18. The communication network according to claim 10, wherein said station and said device further include means for establishing and communicating over a secure connection.

19. The communication network according to claim 18, wherein said secure connection is established through the exchange of authentication keys.

20. The communication network according to claim 18, wherein encrypted flows are used in the establishment of said secure connection.

21. A communication network providing user authentication services, comprising:

n intelligent edge devices, where *n* is a positive integer;

an end system associated with each device, said system having means for communicating with said device;

an authentication server, said server having means for communicating with said device;

means on said device for accepting log-in responses from said system and communicating the accepted log-in responses to said server;

means on said server for comparing for a match the accepted log-in responses with user identification information stored in said network;

means on said server for retrieving authorized connectivity information associated with user identification information which matches the accepted log-in responses; and

means on said server for communicating the retrieved authorized connectivity information to said device.

22. The communication network according to claim 21, further comprising means for accepting and storing, as associated entries, user identification information and authorized connectivity information for particular users.

23. The communication network according to claim 21, wherein said authorized connectivity information defines a set of resources operative within said network.

24. The communication network according to claim 21, wherein said authorized connectivity information include identifiers of one or more virtual local area networks.

25. The communication network according to claim 21, wherein said authorized connectivity information defines a set of resources operative within said network and time restrictions.

26. The communication network according to claim 21, further comprising means on said device for using the communicated authorized connectivity information to establish and implement forwarding and filtering rules for packets transmitted to and from said system.

27. The communication network according to claim 21, further comprising means in said network for generating and storing user tracking information, said user tracking information including information relating to a single log-in attempt.

28. The communication network according to claim 27, wherein said user tracking information includes user identification information and information relating to the location of said system within said network.

29. The secure communication network according to claim 21, wherein said server and said device further include means for establishing and communicating over a secure connection.

30. The secure communication network according to claim 29, wherein said secure connection is established through the exchange of authentication keys.

31. The secure communication network according to claim 29, wherein encrypted flows are used in the establishment of said secure connection.

32. A method for authenticating prospective users of a communication network, comprising:

(a) accepting and storing, as associated entries for particular users, user identification information and lists of network resources, said lists defining sets of resources operative in said network;

(b) accepting log-in responses on an end system in said network;

(c) comparing for a match the accepted log-in responses with the stored user identification information; and

(d) if a match is found, establishing connectivity between said system and the defined set of resources associated with the matching user identification information.

33. A method for authenticating prospective users of a communication network, comprising:

(a) accepting and storing, as associated entries for particular users, user identification information, time restrictions and lists of network resources, said time restrictions defining authorized times, said lists defining sets of resources operative in said network;

(b) accepting log-in responses on an end system in said network during a log-in attempt;

(c) comparing for a user match the accepted log-in responses with the stored user identification information;

(d) upon finding a user match, comparing for a time match the defined authorized times associated with the matching user identification information with the time of the log-in attempt;

(e) upon finding a time match, establishing connectivity between said system and the defined set of resources associated with the matching user identification information for the defined authorized time associated with the matching user identification information.

34. A method for authenticating prospective users of a communication network, comprising:

(a) accepting and storing, as associated entries for particular users, user identification information, lists of network resources and enhanced authentication information, said lists defining sets of resources operative in said network, said enhanced authentication information identifying an enhanced authentication server operative in said network;

(b) accepting log-in responses on an end system in said network;

(c) comparing for a match the accepted log-in responses with the stored user identification information;

(d) if a match is found, conducting an enhanced authentication method between said system and the identified enhanced authentication server identified associated with the matching user identification information; and

(e) if the enhanced authentication method is successfully completed, establishing connectivity between said system and the defined set of resources associated with the matching user identification information.

35. An authentication agent for a network-based user authentication service, comprising:

means for receiving log-in responses from an end system;

means for communicating said log-in responses to an authentication server;

means for receiving authorized connectivity information from said authentication server in response to said log-in responses; and

means for communicating said authorized connectivity information to a processing means, said processing means operative for establishing network connectivity rules for said system using said authorized connectivity information.

36. The authentication agent according to claim 35, further comprising:

means for receiving user status information from said authentication server in response to said log-in responses; and

means for communicating said user status information to said system.

37. The authentication agent according to claim 35, further comprising means for establishing a secure connection for communicating with said authentication server.

38. The authentication agent according to claim 37, wherein said secure connection is established through the exchange of authentication keys.

39. The authentication agent according to claim 35, further comprising means for terminating connectivity with said system after a configurable number of failed log-in attempts.

40. The authentication agent according to claim 35, wherein said authorized connectivity information includes time restrictions defining an access period, and wherein said processing means is operative for abolishing the established network connectivity rules if said access period expires.

41. The authentication agent according to claim 35, wherein said processing means is operative for abolishing the established network connectivity rules if said system becomes disconnected from the network.

42. The authentication agent according to claim 35, wherein said processing means is operative for abolishing the established network connectivity rules if said agent receives from said server a deactivation instruction for said system.

43. The authentication agent according to claim 35, wherein said processing means is operative for abolishing the established network connectivity rules if such system fails to transmit packets for a predetermined length of time.

Add B1